

# Rapid Reference: Embracing Internet Security



## Getting Started -Encryption

### What is Encryption?

Allows your message or request to be sent in a scrambled way during transit so that only you and your recipient can read the message.

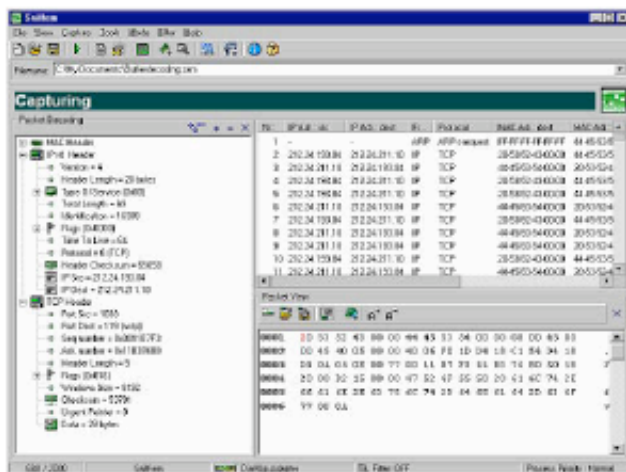
### Encrypt Your Communications

1. **WEP**- Wire Equivalent Privacy-Security protocol for wireless local area networks.
2. **VPN**- Virtual Private Network-Security- a network that uses the public network to transfer information using secure methods.
3. **HTTP vs. HTTPS**: If you are entering information such as credit card numbers or bank account passwords, you will want to use a web site with **https**. This will ensure that the information you entered is encrypted.

<https://>

### Open Wireless Networks

Be careful about how you browse at places that have open wireless networks like wireless libraries and cafe hotspots. These are usually not encrypted and if somebody is on the same network as you, they can use a sniffer (image below) to view information you are sending back and forth (passwords, email, etc.)



### What Makes a Good Password?

1. Does not contain your name or username or any personal information about you.
2. Mix letter and numbers in your password.
3. Use shift (\$@!) characters to make the password harder to crack.

4. Use a phrase as a password spelled with shift characters, numbers, and letters.

**Good Password:** j1/\\_l0v3\$\_c@k3 (jim loves cake)

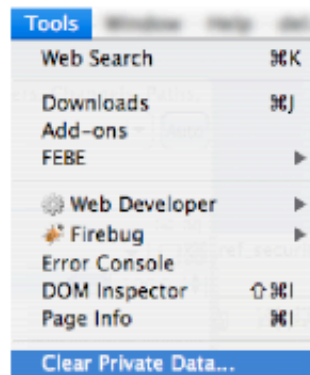
**Bad Password:** jim (Jim's name/username).

### How Do You Clear Private Data from Your Web Browser

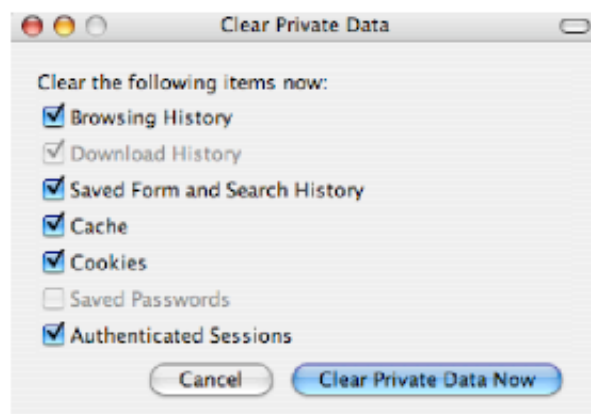
It is a good idea to clear private data from your browser to keep it from becoming available to another subsequent user of that browser. Private data includes passwords, fields filled out in forms, and browser history.

### How to Clear Your Private Data (in Firefox)

1. Go to **Tools menu in Firefox**,
2. Click on **Clear Private Data**.



3. Click the **Clear Private Data button** after you select the items you want to clear.



# Rapid Reference: Embracing Internet Security



## Signing Up For Services Without Using Your Personal Email

A new social network requires that you reveal your email address in order to get set up. What do you do?

### Personal Email Alternatives

1. Set up a **junk email** address to subscribe to service.
2. Use **BugMeNot- You can log in using a shared anonymous username that BugMeNot provides.** There is a Firefox extension for BugMeNot: <http://www.bugmenot.com>.



3. **10 Minute Mail-** Sign up to a service with an email that just lasts 10 minutes: <http://10minutemail.com/>.

### 10 Minute Mail

**Note:** If you did sign up with your personal email, you can always set up filters in your inbox for spam.

### Never Hit Reply or Unsubscribe

**Never hit Reply or Unsubscribe to an email** from a place you **never visited or personally signed up** for. This is a way for spammers to see if your email account is active and legitimate.

### How Do I Protect Myself?

#### Viruses, Worms, and Spyware

1. Keep your virus software **up to date** and your **DAT** files up to date.
2. **Don't click on an email attachment** from somebody you do not know.
3. If your computer starts to run slowly, spyware may be the reason. **Do not click on ads or download programs** that might contain spyware.

#### Trojans

1. **Do not download** anything from **untrusted sources**, such as **file sharing networks**.
2. **Don't click** on a **file in a chat window**.
3. **Don't click on file attachments in email** if it seems fishy. Ask your friend first if they sent you an email with that attachment.

#### Phishing

1. **Never give out personal information** in an **email message**.
2. Before clicking on a **link** to a **webpage** and **entering your username** and **password** on that webpage, make sure the **url in the address bar is correct**.
3. If you receive an **email** from a company that you think **is a fraud**, **contact that company** before doing anything with that email.

#### Social Engineering

1. If **somebody calls you and asks**, **never give out your personal (or anyone else's) information or computer and email passwords**.

#### Sniffing

1. **Do not send unencrypted data** over an open network or open wireless network.
2. Do not **instant message personal and private data**.
3. When **logging into web services** or **entering personal information**, use **HTTPS** (enhanced security) when available.

#### Physical Access to Your Machine

1. **Lock your office** and **log off your computer** when you are finished. (Password protect your computer).
2. **Do not write down passwords** on paper or sticky notes.
3. If **somebody comes to work on your computer**, make sure they have **proper credentials** to do so. **Don't grant physical access** to your machine to just anybody (Prevent keyloggers and USB dumps).

#### Help

If you would like to **know more about Internet Security** or would like to set up group or one-on-one **training** about this topic, please feel free to contact us at **x7489**.